Orin Snyder (*pro hac vice*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc. and Mark Zuckerberg

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: FACEBOOK, INC. CONSUMER PRIVACY USER PROFILE LITIGATION,

This document relates to:

ALL ACTIONS

CASE NO. 3:18-MD-02843-VC

DEFENDANT FACEBOOK, INC.'S OPPOSITION TO PLAINTIFFS' MOTION FOR "LIMITED" DISCOVERY

Table of Contents

Table of Authorities

Cases

Statutes

Rules

I. INTRODUCTION

Plaintiffs' brief reflects a fundamental misunderstanding of how sharing on Facebook works. Ignoring more than a decade of judicial rulings concerning the Internet and social media, Plaintiffs appear to argue that sharing any user data with third-party apps is per se illegal, regardless of user consent. That is not the law—and neither Plaintiffs' motion for discovery nor their 30 individual complaints identify a single viable legal theory or cause of action under which the existence of third-party apps, or the sharing of data with apps, would be unlawful. Nor do Plaintiffs identify a single judicial decision authorizing discovery in this context, where the to-be-operative complaint has not yet been filed, the plaintiffs are peddling an untested theory of liability, and the defendant has identified significant concerns regarding the viability of the lawsuit.

At the recent CMC, this Court repeatedly asked Plaintiffs to explain how their factual allegations amount to civil liability against Facebook. None of the Plaintiffs could articulate a plausible theory of standing. And during the July 31, 2018 telephonic conference, the Court asked Plaintiffs to explain in their motion why the discovery they seek "would go to the core of what [they] will be alleging in [their] amended complaint." July 31, 2018 Tr. at 14. Despite this instruction, Plaintiffs still do not specify what claims they will be alleging, much less how their allegations state a claim or how the discovery they seek will further those claims. This silence confirms that Plaintiffs have no viable claim, and they should not be permitted to embark on a futile effort to find one. Discovery should not commence unless and until they show they can state a valid claim.

Facebook users *consent* to sharing their data with third-party apps. The explanation that Plaintiffs *do* offer makes clear that they do not understand Facebook or the role that apps and user consent play in this context. Since 2007, apps have been an important feature for Facebook users, not a bug. More than 80 million apps are integrated with Facebook's platform today. Apps like CNN allow people to share news articles with family. Apps like Words with Friends allow people to play games with their friends. Some apps, like Paypal, allow people to make payments to each other. Others, like Spotify, allow people to discover their friends' favorite music. Integrating apps with Facebook enhances the user experience by enabling people to bring their friends with them and customize their experience with a single log-in.

Facebook users (like users of apps on other platforms) consent to their data being shared with third-party apps or have the option to turn off such sharing entirely. Facebook's terms of service and data use policy, both of which are referenced in the complaints and discussed in Plaintiffs' motion, make this expressly and abundantly clear. And with respect to the sharing of data with apps *by a user's Facebook friends*, that was also done *only* with the consent of the user whose data was shared (until that feature was eliminated in 2015), as the same documents made clear. This same paradigm applies to other Internet platforms, including Apple, Google, Twitter, and many others; users consent to the sharing of their information, on terms they largely control, to get a more personalized and social experience. The problem with Cambridge Analytica was *not* that Facebook shared data without user consent—all users did consent—but that the app developer, Aleksandr Kogan, obtained the user data and sold it to Cambridge Analytica in violation of Facebook's policies. Numerous articles describing those events, including articles cited by Plaintiffs themselves, make this crystal clear,[1] and Plaintiffs' own complaints are in accord.[2] This is why Plaintiffs' counsel has admitted that this is not a data breach case, in which users' data was obtained against their will.[3] And if Plaintiffs disagree that people should be permitted to consent to sharing their data with apps, their remedy is not in the courts where they have no viable claim. *See Henson v. Santander Consumer USA Inc.*, 137 S. Ct. 1718, 1725–26 (2017).

---

[1] *See, e.g.*, Ex. A, Cadwalladr & Graham-Harrison, *Revealed: 50 Million Facebook profiles harvested for Cambridge Analytica in major data breach* ("Facebook's 'platform policy' allowed only collection of friends' data to improve user experience in the app and barred it being sold on or used for advertising."); Ex. B, Cadwalladr & Graham-Harrison, *How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool* ("Kogan did not have permission to collect or use data for commercial purposes. His permission from Facebook to harvest profiles in large quantities was specifically restricted to academic use. And although the company at the time allowed apps to collect friend data, it was only for use in the context of Facebook itself, to encourage interaction. Selling that data on, or putting it to other purposes—including Cambridge Analytica's political marketing—was strictly barred.").

[2] *See* Haslinger Compl. ¶¶ 17–18 (alleging that Facebook users who had their data collected by the thisisyourdigitallife app either consented to the collection of data directly with the app or "had their privacy setting set to allow it."); Beiner Compl. ¶ 40 (acknowledging that "Facebook's Privacy Policy *does* address the phenomenon of third-party apps being able to acquire user information via that user's friends" and quoting the policy); Johnson Compl. ¶ 53 (acknowledging that Facebook's privacy settings disclosed that "People on Facebook who can see your info can bring it with them *when they use apps*. … Use the settings below to control the categories of information that people can bring with them *when they use apps, games and websites*.").

[3] *See* Dkt. 64 (Steve Berman Ltr.) ("[T]his is not a data-breach case such as *Anthem* or *Adobe Systems*. It does not concern a breach aimed at stealing Social Security numbers, credit-card numbers, or other financial data. Hackers did not break in through the back door.").

Plaintiffs *lack standing* because they have not suffered any Article III injury. Despite repeated colloquies with the Court about the challenge of proving standing and whether users suffered any concrete or particularized harm, Plaintiffs' brief does not articulate *any* harm suffered by *any* Facebook user—let alone the named Plaintiffs themselves. The reason is simple: No Facebook user suffered Article III injury as a result of the Cambridge Analytica events or the sharing of data with any other (as yet, unidentified) third-party apps. Where Article III standing is this lacking, and Plaintiffs do nothing to demonstrate that they will have viable answers, discovery should not commence.

The "limited" discovery Plaintiffs seek is *staggeringly broad*. The discovery Plaintiffs want would encompasses *every* app that has *any* data about *any* Facebook user since the launch of the platform in 2007—potentially tens of millions of them. Indeed, the term "third parties" in the discovery requests would arguably include *all* individual Facebook users who have access to any user data—in other words, all 2.8 billion users of Facebook worldwide, as well as billions of other Internet users who are not on Facebook but who can see content on Facebook that is public. That is absurd. There is nothing unlawful about Facebook or apps and no reason for this Court to sanction Plaintiffs' obvious fishing expedition. And Plaintiffs' professed desire to learn how much revenue Facebook generates from apps reflects a willful disregard for how Facebook works. Offering an app on or integrating an app with Facebook is *free*. Facebook does not "sell" user data or access thereto, as Plaintiffs know.[4]

Plaintiffs seek this astonishingly broad discovery before they have even filed a consolidated complaint specifying what theories they will pursue and on whose behalf. This approach runs headlong into the Federal Rules, which "contemplate pre-complaint discovery only in very limited circumstances not applicable here." *In re Flash Memory Antitrust Litig.*, 2008 WL 62278, at *5 (N.D. Cal. Jan. 4, 2008). "[T]he timing of discovery under" those Rules "is not a mere formalism," as the existence of an operative complaint is the very "basis for court resolution of discovery disputes." *Id*. Absent an

[4] Facebook charges a fee for processing users' payments made on its platform (which is disclosed in its public securities filings). But Plaintiffs' assertion that "Facebook sells users' [Personal Data] to unidentified third parties" is false. Mem. at 3; *see also id*. at 2 ("Third parties … have paid Facebook to access [users' Personal Data] include media companies … and any number of other companies."); *id*. at 6 ("The facts already known support claims … of Facebook's deliberate participation in collecting and disseminating highly personal information to third parties for profit and without informed consent."). Facebook expects that false statements like these will not appear in the consolidated complaint, since there is no factual basis for them and they could not be alleged consistent with Plaintiffs' Rule 11 obligations.

operative complaint—and absent any showing that Plaintiffs will be able to plead *any* viable claims against Facebook—Plaintiffs should not be permitted to use "[d]iscovery … as a substitute for an adequate pleading," or "to launch a fishing expedition." *Optical Coating Lab., Inc. v. Applied Vision, Ltd.*, 1995 WL 150513, at *4 (N.D. Cal. Mar. 20, 1995).

II. BACKGROUND

A. Facebook's Platform and Third-Party Apps

Facebook began as a social networking site for college students in 2004. Its founder, Mark Zuckerberg, saw that the service had the potential to transform how people interacted with each other on the Internet. In November 2007, Facebook launched its "Platform," a way for third-party developers to offer applications ("apps") that, among other things, provide social experiences based on the connections people make on Facebook. (Apple launched its App Store months later in July 2008, and Google followed with Android Market in August 2008.) There are now tens of millions of third-party apps that people use across these and many other platforms.

Facebook's Data Use Policy informs users of the information apps may access if they choose to use (or "authorize") them. For example, the version of Facebook's Data Use Policy in effect in 2013 and 2014[5] told users that apps they accessed would receive their User ID—a string of numbers associated with a particular user (not to be confused with the Facebook ID)—and any information that user shared publicly. *See* Ex. C at 8. Apps could also access users' friends' User IDs, also called a "friend list." *Id*. As the Data Use Policy explained, providing this information to apps allowed users to obtain the social benefits of connecting the apps to Facebook. *Id*. at 9. Providing a friend list "lets [users] find [their] friends on that application," and a "User ID helps the application personalize [a user's] experience." *Id*. Again, Facebook provided a setting that enabled people to turn off all Platform apps, and not share their data in this fashion.

Earlier versions of Facebook's Platform also allowed users to share some additional information about their friends. For example, as the Data Use Policy in effect in 2013 and 2014 informed users, "one of your friends might want to use a music application that allows them to see what their friends

[5] The version of Facebook's Data Use Policy contained in Exhibit C was revised on November 15, 2013. All portions of the policy cited here are substantially similar to the prior version from 2012.

are listening to." Ex. C at 9. In using the app, "[y]our friend might … want to share the music you 'like' on Facebook." *Id*. "If you have made that information public, then the application can access it just like anyone else. But **if you've shared your likes with just your friends, the application could ask your friend for permission to share them**." *Id*. (emphasis added). Thus, a user's friend could re-share a friend's likes with an app the user had downloaded, so long as the original friend (whose likes were at issue) had consented to such sharing. If that user had chosen to turn off all Platform apps, that person's friends could not share it.

B. Data use and sharing on Facebook is governed by a series of agreements

As Plaintiffs acknowledge, Facebook users must "agree[] to Facebook's terms of service and a code of conduct, among other requirements," before they gain access to Facebook. Mem. at 2. In 2013 and 2014, when the alleged sharing of the data at issue here took place, a user's agreement with Facebook was governed by two primary documents, Facebook's Statement of Rights and Responsibilities ("SRR") and its Data Use Policy. *See, e.g.*, Burk Compl. ¶ 85 ("Plaintiffs and Class members had agreements with Facebook, including Facebook's Data Use Policy and its Statement of Rights and Responsibilities.").[6] The SRR stated that "[b]y using or accessing Facebook, you agree to this Statement," and informed users that Facebook's Data Policy governed "how [Facebook] collect[s] and can use your content and information." Ex. D.[7]

The terms of these agreements covered what information Facebook, Facebook users' friends, the public, applications, and service providers could access. The first full sentence of the Data Use Policy in effect in 2013 and 2014 stated that Facebook "receive[s] a number of different types of information about you," including "the information you choose to share on Facebook, such as when you

[6] Any consolidated complaint Plaintiffs file necessarily will incorporate these policies, as does Plaintiffs' brief. Mem. at 1–2. Many of the complaints cite these documents, *see, e.g.*, Beiner Compl. ¶ 38; Burk Compl. ¶ 85; Picha Compl. ¶ 35; Reninger Compl. ¶ 29, and all ground their claims on alleged promises or representations in them. Courts may take into account such documents even when they are not physically attached to the complaint. *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1160 (9th Cir. 2012) (citation omitted). Even where the complaint does not explicitly refer to a document, the document is incorporated where its contents are "integral" to the claims. *See Coto Settlement v. Eisenberg*, 593 F.3d 1031, 1038 (9th Cir. 2010). The Court need not accept as true conclusory allegations that are contradicted by documents referenced in the complaint. *Steckman v. Hart Brewing Inc.*, 143 F.3d 1293, 1295–96 (9th Cir. 1998).

[7] Facebook's current Terms of Service likewise inform users that they "must agree to" Facebook's Data Policy to use Facebook. *See Terms of Service*, Facebook (April 19, 2018) https://bit.ly/1cwZ2RJ.

post a status update, upload a photo, or comment on a friend's story." Ex. C at 2. Facebook uses this data "to serve [users] ads or other content" and "in connection with the services and features [Facebook] provides to … [its] partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use." *Id*. at 3–4. The Policy also stated that Facebook "may allow service providers to access information so they can help [Facebook] provide services." *Id*. at 5. These service providers, which included mobile devices, were required to "only use … information consistent with the agreement [Facebook] enter[ed] into with them, as well as th[e] Data Use Policy." *Id*. at 15.

The Data Use Policy also disclosed that the information users share with friends may be disclosed to the apps their friends use: "Just like when you share information by email or elsewhere on the web, information you share on Facebook can be re-shared. This means that if you share something on Facebook, anyone who can see it can share it with others, including the games, applications, and websites they use." Ex. C at 9. Elsewhere, users were reminded that, even if they deleted their apps, "apps may still be able to access your information when the people you share with use them." *Id*. And the Policy told users that they could prevent friends from sharing their information with apps: "You can control most of the information other people can share with applications they use from the 'Apps' settings page." *Id*. And "if you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications." *Id*.

Facebook's policies also restricted how app developers could use data obtained from Facebook users. Among other limitations, Facebook's Platform Policies required developers to not "sell user data" or "directly or indirectly transfer any data … [to] any ad network, ad exchange, data broker, or other advertising related toolset, even if a user consents." Ex. D at 2–3.

C. Facebook changes the Platform to limit the data apps could access

In April 2014, Facebook announced a new version of its Platform. Ex. E at 4. Among other changes, third-party apps could no longer ask for data about a person's friends (unless, of course, a friend him- or herself chose to use the app). Existing apps were given a one-year grace period until April 2015 to migrate to the new version of the Platform.

D. Kogan and Cambridge Analytica violate Facebook's policies

On December 11, 2015, the *Guardian* reported that the campaigns of presidential candidates Ted Cruz and Ben Carson had used Facebook data compiled by Cambridge Analytica to target potential voters. Ex. F (cited at, e.g., Beiner Compl. ¶ 27 n.14). The article reported that a Cambridge-based lecturer named Aleksandr Kogan had created an app that paid Facebook users to take a "personality questionnaire" using their Facebook log-in, in order to access their names, locations, birthdays, genders, and Facebook "likes." *Id*. at 3. The app had been created in 2013, before Facebook changed the Platform, and it was installed by around 300,000 people. Ex. E at 3. Kogan was also able to access some data of tens of millions of these users' friends, provided that the privacy settings of the users *and their friends* allowed such access. *Id*. Kogan later sold some of the data to Cambridge Analytica in violation of Facebook's rules. *Id*. at 4.

In response to the 2015 *Guardian* article, Facebook immediately demanded that Kogan and Cambridge Analytica delete all Facebook user information they had obtained. Ex. E at 4. Soon after, Facebook permanently banned Kogan's app. *Id*. Facebook also demanded that Kogan, Cambridge Analytica, and Christopher Wylie (a former employee of Cambridge Analytica) certify that they had deleted the improperly-acquired data. They each certified in writing that they had done so. *Id*.; Ex. G.

In March 2018, Facebook learned from the *Guardian*, the *New York Times*, and Channel 4 that, according to Christopher Wylie, Cambridge Analytica, Kogan, and/or Wylie may not have deleted the data as they had certified. Facebook immediately banned them from using any of its services. Ex. E at 4. Cambridge Analytica continued to claim it had already deleted the data and agreed to a forensic audit by a firm Facebook hired to confirm the data's deletion. *Id*. That audit was suspended when the relevant investigatory body in the U.K., the Information Commissioner's Office, began its own investigation and directed Facebook to halt its audit. *See Pursuing Forensic Audits to Investigate Cambridge Analytica Claims*, FACEBOOK (Mar. 19, 2018), https://bit.ly/2FUFxGN. In May 2018, Cambridge Analytica and affiliated entities filed for bankruptcy in the U.K. and United States.

In the wake of these news reports, dozens of lawsuits were filed against Facebook, all focusing on the Cambridge Analytica/Kogan events. The Judicial Panel on Multidistrict Litigation ultimately

transferred the lawsuits to this Court on the basis that all of the actions alleged that "Cambridge Analytica and other [related] defendants exploited Facebook's platform to obtain user data." MDL No. 2843, Dkt. 140 (June 6, 2018).

III. ARGUMENT[8]

A. The Court should stay discovery pending resolution of Facebook's motion to dismiss

Good cause exists to stay discovery where, "absent discovery," a pending motion may resolve "potentially dispositive" issues. *Carter v. Oath Holdings, Inc.*, 2018 WL 3067985, at *4 (N.D. Cal. June 21, 2018); *Gibbs v. Carson*, 2014 WL 172187, at *3 (N.D. Cal. Jan. 15, 2014); *Hamilton v. Rhoads*, 2011 WL 5085504, at *1 (N.D. Cal. Oct. 25, 2011); *see also Jarvis v. Regan*, 833 F.2d 149, 155 (9th Cir. 1987); *cf. Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 558 (2007) (where "complaint … could not raise a claim of entitlement to relief, 'this basic deficiency should … be exposed at the point of minimum expenditure of time and money'" (citation omitted)).

Although "the court must take a 'preliminary peek' at the merits of the" defendant's dismissal arguments "to assess whether a stay is warranted," *Carter*, 2018 WL 3067985, at *4, it need not reach any definitive conclusion regarding the merits. Rather, courts in this Circuit stay discovery where there is a "clear *possibility*" that a dispositive motion will be granted. *See, e.g.*, *GTE Wireless, Inc. v. Qualcomm, Inc.*, 192 F.R.D. 284, 287 (S.D. Cal. 2000) (emphasis added). A stay is particularly appropriate where the "[d]efendant challenges Plaintiffs' Article III standing," *see Camacho v. United States*, 2014 WL 12026059, at *3 (S.D. Cal. Aug. 15, 2014); *Al Otro Lado, Inc. v. Nielsen*, 2018 WL 679483, at *3 (S.D. Cal. Jan. 31, 2018). That is because Article III standing is jurisdictional and, therefore, is a threshold inquiry. *Bates v. United Parcel Serv., Inc.*, 511 F.3d 974, 985 (9th Cir. 2007) (en banc). A motion for a stay need not resolve every claim; a stay is warranted where a motion to dismiss may "limit the scope of discovery" by resolving some of the issues in the case. *In re Nexus 6p Prod. Liab. Litig.*, 2017 WL 3581188, at *2 (N.D. Cal. Aug. 18, 2017).

[8] This Opposition is based on claims pled to date and is not intended to be an exhaustive list of possible defenses or flaws in Plaintiffs' forthcoming consolidated class action complaint.

1. Facebook's motion to dismiss is likely to dispose of Plaintiffs' claims because they consented to the policies they attack.

According to Plaintiffs, the "consistent" "gravamen of the claims" here is that "Facebook collected Plaintiffs' Personal Data and disseminated it … without notice and in violation of any terms of agreement." Mem. at 1. All of Plaintiffs' claims fail as a matter of law because the very agreements they cite establish that Plaintiffs were informed of, and consented to, Facebook's policies governing who may access users' data, the types of data that may be accessed, and under what conditions.

As Plaintiffs acknowledge, Facebook users must agree to abide by Facebook's terms before they access Facebook. Mem. at 2 (users "agree[] to Facebook's terms of service and a code of conduct, among other requirements"); *see also* Burk Compl. ¶ 85 ("Plaintiffs and Class members had agreements with Facebook, including Facebook's Data Use Policy and its Statement of Rights and Responsibilities."). These agreements foreclose Plaintiffs' claims. Among other terms, Plaintiffs agreed that:

- The Data Use Policy would govern the types of information Facebook collects and how that information is used, all of which were clearly disclosed, *see* Ex. C;
- Facebook could allow service providers to access information in order to help Facebook provide services, *id*. at 5;
- Friends could re-share information with apps if users' privacy setting allowed it, *id*. at 9;
- To completely block apps from getting their data, they need to turn off Platform apps, *id*.;
- How third-party apps treated their data was governed by the apps' privacy policies, *id*. at 8.

See supra pages 4–6. A number of courts have dismissed claims, including claims against Facebook, where users explicitly consented to conduct disclosed in the defendant's terms of service. *See Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953 (N.D. Cal. 2017); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028–32 (N.D. Cal. 2014). And courts regularly uphold Facebook's terms of service and other policies in dismissing litigation against Facebook. *See, e.g.*, *Cross v. Facebook, Inc.*, 14 Cal. App. 5th 190, 203–04 (2017) (dismissing case where "the actual terms are to the contrary" of Plaintiff's theory); *Klayman v. Zuckerberg*, 753 F.3d 1354, 1359 (D.C. Cir. 2014) ("[T]he plain text of [Facebook's SRR] disavows the legal relationship that [plaintiff] asserts."). Plaintiffs' claims are barred by Facebook's terms and policies.

2. Plaintiffs lack Article III standing because they have not suffered a concrete and particularized injury

All of Plaintiffs' claims also fail because they lack standing to bring them, a dispositive issue this Court flagged at the initial CMC. Dkt. 98 at 9. To satisfy the "irreducible constitutional minimum of standing," Plaintiffs must establish an injury that is: (1) concrete and particularized, and actual or imminent, not conjectural or hypothetical; (2) causally connected to the defendant's alleged wrongdoing; and (3) redressable. *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992). "A 'concrete' injury must be '*de facto*'; that is, it must actually exist," and cannot be "abstract." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). It is insufficient to plead a mere statutory violation; "'a bare procedural violation …, divorced from any concrete harm' will not constitute an injury-in-fact." *Dutta v. State Farm Mut. Auto. Ins. Co.*, 895 F.3d 1166, 1173 (9th Cir. 2018) (quoting *Spokeo*, 136 S. Ct. at 1549). Of course, in light of the fact that Plaintiffs consented to sharing their data with the apps they and their friends used, standing cannot be premised on any alleged infringement of Plaintiffs' privacy. *See e.g.*, *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072 (N.D. Cal. 2016) ("[A] plaintiff cannot have a reasonable expectation of privacy if she consented to the intrusion."). But even with the various allegations of "harm" discussed in Plaintiffs' complaints, the allegations confirm that Plaintiffs have not suffered the kind of concrete injury sufficient to support standing.

Plaintiffs cannot plausibly allege that the market value of their personal information was diminished. Several of the complaints claim that Plaintiffs suffered an economic loss because they "own" their data and the data allegedly has a "fair market value."[9] Plaintiffs' motion even makes the dubious assertion that their data is worth "billions of dollars." Mem. at 1–2. But "injury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff's personal identification information." *In re Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5 (N.D. Cal. Dec. 3, 2013). "'Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers,' but courts have not held that 'the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.'" *Goodman v. HTC Am., Inc.*, 2012 WL 2412070, at *7 (W.D. Wash. June 26, 2012) (citation omitted). Rather, "a plaintiff must

[9] *See, e.g.*, Gerena Compl. ¶ 69; O'Kelly Compl. ¶ 51; Sanchez Compl. ¶ 78; Schinder Compl. ¶ 68.

allege how the defendant's use of the information deprived the plaintiff of the information's economic value." *Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *5. Plaintiffs have not made, and cannot make, such a showing. Plaintiffs "do not allege they attempted to sell their personal information, that they would do so in the future, or that they were foreclosed from entering into a value for value transaction relating to their PII, as a result of [Facebook's] conduct." *In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236, at *4 (N.D. Cal. Mar. 26, 2013). They therefore have not alleged any concrete economic loss. *See Low v. LinkedIn Corp.*, 2011 WL 5509848, at *4–5 (N.D. Cal. Nov. 11, 2011); *In re iPhone Application Litig.*, 2011 WL 4403963, at *4 (N.D. Cal. Sept. 20, 2011); *LaCourt v. Specific Media, Inc.*, 2011 WL 1661532, at *4 (C.D. Cal. Apr. 28, 2011).

Plaintiffs cannot plausibly allege that the disclosure of information they shared on Facebook placed them at an increased risk of identity theft. Another theory of injury advanced in some complaints is that Cambridge Analytica's alleged acquisition of Plaintiffs' data placed them at an increased risk of identity theft.[10] Multiple courts have rejected this approach, holding that a plaintiff does not allege injury in fact where he does not allege that data such as social security numbers or credit card information was disclosed. *See, e.g.*, *In re SuperValu, Inc.*, 870 F.3d 763, 769–71 (8th Cir. 2017); *Dugas v. Starwood Hot. & Res. Worldwide, Inc.*, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016); *Antman v. Uber Techs., Inc.*, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015).

Plaintiffs do not allege that the data at issue here could be used to steal someone's identity. Nor would any such allegation be plausible. The information was, by definition, shared by Plaintiffs with numerous people on Facebook, including the friends who shared it with Kogan's app, and did not include information that could be used to engaged in identity theft, "such as social security numbers, account numbers, or credit card numbers." *Antman*, 2015 WL 6123054, at *11. Plaintiffs do not allege that identity thieves obtained any information, or offer any cogent explanation of how they might do so. Nor can they bootstrap standing by claiming that they suffer anxiety about what harms might befall them in the future as a result of the alleged disclosure. Plaintiffs "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 416 (2013); *see also Beck v. McDonald*, 848 F.3d 262, 272 (4th Cir.), *cert.*

[10] *See, e.g.*, Haslinger Compl. ¶ 88; Skotnicki Compl. ¶ 80; Sanchez Compl. ¶ 78.

denied sub nom. Beck v. Shulkin, 137 S. Ct. 2307 (2017).

Plaintiffs cannot "articulate a sufficient contract injury" amounting to injury in fact. *See Google, Inc. Privacy Policy Litig.*, 2013 WL 6248499, at *6. "Nominal damages are not available in California for breach of contract," and "a contract breach by itself [does not] constitute[] an injury in fact." *Id.*; *accord Meneses v. U–Haul Int'l, Inc.*, 2012 WL 669518, at *5 (N.D. Cal. Feb. 29, 2012); *Frangipani v. Boecker*, 64 Cal. App. 4th 860, 865 (1998) (contract damages "not recoverable for mental suffering or injury to reputation"). Yet Plaintiffs cannot plausibly allege any existing or threatened harm from the alleged disclosures, for the reasons set forth above.

In any event, to plead a breach of contract claim, Plaintiffs must "allege the specific provisions in the contract creating the obligation [Facebook] is said to have breached." *Young v. Facebook, Inc.*, 790 F. Supp. 2d 1110, 1117 (N.D. Cal. 2011). Plaintiffs' sole theory is that Facebook had an obligation to prevent Cambridge Analytica and third-party apps from obtaining their data. Mem. at 1. But neither the Data Use Policy nor the SRR creates such an obligation, and in fact, their terms are to the contrary. Plaintiffs explicitly agreed that, absent adjustments to their privacy settings, friends may share their information with apps. And far from legally obligating Facebook to prevent third-party misconduct, the Data Use Policy told users that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook" (Ex. C at 8) and the SRR stated that a user's "agreement with [an] application will control how the application can use, store, and transfer … content and information." Ex. D at 1. In addition, the SRR clearly and unambiguously waived claims based on third-party conduct. It stated,

> FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES.

Ex. D at 4. This provision also expressly waived California Civil Code § 1542. *Id.* Plaintiffs' claims against Facebook arise directly out of—and are plainly "connected with"—the misconduct of third parties like Kogan and Cambridge Analytica.

Numerous other flaws permeate the claims in their Plaintiffs' complaints, all of which can be resolved without discovery on a motion to dismiss. These fatal defects are outlined in an Appendix at

the end of this Memorandum. *See Carter*, 2018 WL 3067985, at *3–4 ("court must take a 'preliminary peek' at the merits of the" defendant's dismissal arguments "to assess whether a stay is warranted"). Given the dispositive legal deficiencies in their prior complaints, Plaintiffs should be required to present viable theories against Facebook before they can impose "the burdens of discovery." *Ashcroft v. Iqbal*, 556 U.S. 662, 672 (2009).

B. Plaintiff cannot show good cause for pre-complaint discovery

Plaintiffs' absurdly overbroad discovery requests must be denied because Plaintiffs offer no good cause to ignore the ordinary rule barring discovery before a complaint has been filed. *See Flash Memory*, 2008 WL 62278, at *3. The Federal Rules "contemplate pre-complaint discovery only in very limited circumstances not applicable here." *Id*. at *5. "[T]he timing of discovery under the Federal Rules is not a mere formalism," as "[a]llowing discovery outside the terms of the[] Rules, and before an operative complaint is filed, obviates the [Rules'] protections" (*id*.) by depriving the parties and the Court of any means of measuring how the discovery sought relates to Plaintiffs' claims. Although a plaintiff may "take discovery to find evidence to support a properly pleaded claim for relief[,] a plaintiff is not permitted to take discovery to fish for claims." *Kinetic Co. v. Medtronic, Inc.*, 2011 WL 1485601, at *4 (D. Minn. Apr. 19, 2011). Indeed, this Court said as much at the CMC, noting that Plaintiffs should not attempt "to … discover claims that … [they] wouldn't be able to assert without the [pre-complaint] discovery." Dkt. 98 (Tr. of July 19, 2018 CMC) at 31–32. Yet Plaintiffs make no secret of the fact that the purpose of their extraordinarily broad requests is to discover what they "do not know, but wish to know, before filing a pleading." Mem. at 11.

Plaintiffs have tried to peddle the theory that pre-complaint discovery is "standard practice" in large class actions. Dkt. 98 (Tr. of July 19, 2018 CMC) at 12; Mem. at 9–10. That is simply wrong. Even where a complaint has been filed, generally a "party may not seek discovery from any source before the parties have conferred as required by Rule 26(f)." Fed. R. Civ. P. 26(d)(1). "Courts may authorize early discovery only if the moving party shows 'good cause' for deviating from the standard discovery timetable," *United States ex rel. Brown v. Celgene Corp.*, 2014 WL 12588280, at *1 (C.D. Cal. Mar. 21, 2014), and do so "only in narrow circumstances." *Sky Angel U.S., LLC v. Nat'l Cable Satellite Corp.*, 296 F.R.D. 1, 2 (D.D.C. 2013). In evaluating good cause, courts consider (1) whether

a preliminary injunction is pending; (2) the breadth of the requests; (3) the plaintiff's purpose for requesting early discovery; (4) the burden of compliance; and (5) how far in advance of the typical discovery process the requests were made. *Celgene*, 2014 WL 12588280, at *1. None of these factors supports Plaintiffs' extraordinarily broad requests, and granting them at this early juncture—when there are serious doubts about whether Plaintiffs have viable claims—would be unprecedented.

1. There is no preliminary injunction pending.

"[T]here is no pending motion for a preliminary injunction in this case" so "there is simply no urgent need for the requested discovery." *Celgene*, 2014 WL 12588280 at *2. Although Plaintiffs claim "irreparable ongoing harm" (Opp. at 4), they do not describe that harm, or explain how their requests would help prevent it.

2. Plaintiffs' requests for discovery are burdensome and massively overbroad.

Plaintiffs' extraordinarily broad discovery requests reflect the scattershot and incoherent nature of their claims. They seek (among other things) the identity of every person or company who has ever developed one of the tens of millions of Facebook apps, as well as information about every person or company that has access to any Facebook user information, which could include nearly everyone on the Internet. It is unclear how this information would help them identify wrongdoers or obtain evidence in support of their claims—whatever these claims may be. Indeed, without the benefit of a complaint, one cannot know how the requests relate to Plaintiffs' contemplated claims at all.

Plaintiffs' First Request asks Facebook "to identify all apps, app developers, and other third parties … that Facebook has identified as having accessed or obtained the Personal Data of Facebook users." Not. of Mot. at 1. It defines "Personal Information" broadly to include, among other things, "information linked to [an] individual," *id*. n.1, and therefore includes all data that Facebook users share on the platform, including public information. ***This request would reach every app.*** As Facebook's current Data Policy states, "[p]ublic information can … be seen, accessed, reshared or downloaded … by apps, websites and other services that integrate with [Facebook]." Data Policy (Aug. 3, 2018), https://bit.ly/1Dwr7Vp. And, users can choose to share additional information with apps beyond what is shared on their public profile. *Id*. Read literally, the request could cover the entire Internet, as it asks Facebook to identify "third parties" with access to any sort of information Facebook collects,

including public information. This request has no connection to Plaintiffs' claims, and offers no insight into whether anyone misused Plaintiffs' data.

Plaintiffs' Second Request seeks "any agreements between Facebook and each of the apps, app developers, and other third parties identified in Category 1." Not. of Mot. at 1. It therefore seeks agreements with tens of millions of apps, because every app on Facebook accesses some information about the user who installed it, and thus has no connection to Plaintiffs' claims. The request also seeks information about "payments" Facebook received from all of these apps, broken down by quarter, over a span of nearly ten years. As noted above, Facebook charges a fee for processing users' payments on its Platform (and those figures are disclosed publicly), but offering an app on Facebook is free and Facebook does not sell user data.

Plaintiffs' Third Request seeks "[f]or each of the apps, app developers, and other third parties identified in Category 1, a written description of each type of Personal Data, described categorically, that Facebook has identified as having been accessed or obtained." Not. of Mot. at 2. This request appears to seek a list of all types of personal information an app could conceivably obtain. But the information to which apps could request access is covered in Facebook's relevant data policies, which are already in Plaintiffs' possession. Moreover, a generic list of the types of personal information apps could obtain would not help Plaintiffs identify wrongdoing.

Plaintiffs' Fourth Request seeks information regarding "how each app, app developer, and any other third parties" accessed or obtained the Personal Data of Facebook users. Not. of Mot. at 2. This request is overbroad for the same reasons as Plaintiffs' first three requests, as it seeks information about tens of millions of apps and untold numbers of third parties who accessed Facebook data through entirely legitimate channels. To the extent it seeks information about Facebook's own policies vis a vis the apps, those policies (including the SRR and Platform Policies) are publicly available. And, once again, the impossibly broad undertaking Plaintiffs seek to impose on Facebook would not help them to identify wrongdoers, since apps could only access user data with users' consent.

Plaintiffs' Fifth Request asks Facebook to "identify how each app, app developer, and any other third party used the Personal Data it accessed or obtained." Not. of Mot. at 2. This request is

overbroad because it, too, seeks information about the inner workings of tens of millions of apps developed by third parties. How each app uses the data it obtains through legitimate channels to provide its services is unique to each app, and such information would not help Plaintiffs identify wrongdoing. To the extent Plaintiffs seek information about allegedly secret *misuse* of Facebook data (if any), that information would be in the possession of the third parties who developed the apps.

Plaintiffs' Sixth Request asks for "each version of each form of communication that in or since March 2018 has been transmitted to Facebook users relating to whether Facebook users' Personal Data was accessed or obtained by apps, app developers, and other third parties." Not. of Mot. at 2. It is unclear why Plaintiffs need these communications; if Plaintiffs are among the users whose data may have been accessed by Cambridge Analytica, they should have received such communications.

3. Plaintiffs' request for all documents produced to all regulators in the U.S. and U.K. is improper, overbroad, and cannot be evaluated without a complaint

Plaintiffs' Seventh Request seeks "all documents provided to federal and state regulators in the United States, and regulators in the United Kingdom, in response to inquiries and investigations of the conduct alleged in the underlying complaints." These requests are improper and wildly overbroad.

Plaintiffs have no "right of access to ongoing government investigations" or entitlement "to the work of … regulatory investigators," and must "fashion their own document requests without relying upon the government subpoenas." *In re WorldCom, Inc. Sec. Litig.*, 2003 WL 22953645, at *7 (S.D.N.Y. Dec. 16, 2003). "[T]he compelled act of turning records over to the government … does not mean that everyone else has an equal right to rummage through the same records." *In re Graphics Proc. Units Antitrust Litig.*, 2007 WL 2127577, at *5 (N.D. Cal. July 24, 2007). Rather, "[t]he traditional route for obtaining document discovery is to serve subject-matter-specific requests for production, which 'must describe with reasonable particularity each item or category of items to be inspected.'" *In re Volkswagen "Clean Diesel" Mktg., Sales Practices, & Prods. Liab. Litig.*, No. 15-md-2672-CRB, Dkt. 4996 at 2 (N.D. Cal. Apr. 24, 2018) (quoting Fed. R. Civ. P. 34(b)(1)(A)). "Such '[d]irect requests allow a court to consider the relevance of the information sought to the specific claims and defenses in the pending case.'" *Id.* (quoting *Wollam v. Wright Med. Grp., Inc.*, 2011 WL 1899774, at *2 (D. Colo. May 18, 2011)). Where "a party seeks discovery of documents that were produced during other litigation or investigations, a different—hazier—analysis ensues." *Id.* Here, because "the

Court does not know the precise contours of the government investigations at issue," "[t]he document requests or subpoenas issued by the … agencies … are not before the Court," and the "investigations are confidential and ongoing," it is impossible to "adequately determine how the scope of those investigations compares to that of [Plaintiffs'] case, let alone determine whether all of the documents produced … in those investigations are relevant to the[ir] claims." *Id*. That is particularly true because Plaintiffs have not even filed a consolidated complaint identifying their claims. "[S]uch an approach makes it difficult"—if not impossible—"to ensure that the scope of discovery is not expanded beyond what is allowed by the Federal Rules." *Id*. at 3; *see also King Cty. v. Merrill Lynch & Co.*, 2011 WL 3438491, at *3 (W.D. Wash. Aug. 5, 2011).

Because any productions to investigators would have occurred outside the strictures of the Federal Rules, Facebook could not simply re-produce the documents. It would have to review them again, which would require substantial time and expense. Facebook would undoubtedly have "various objections … that might be assertable against plaintiffs that were unasserted against the government." *Graphics Proc. Units*, 2007 WL 2127577, at *5. Plaintiffs are therefore wrong that "[t]here is no burden associated with" producing documents previously produced to the government (Mem. at 11), because "documents previously produced in government investigations or other litigation may in fact be irrelevant to the claims asserted in *this* case." *In re Countrywide Fin. Corp. Deriv. Litig.*, 542 F. Supp. 2d 1160, 1180 & n.29 (C.D. Cal. 2008).

Compelling this extraordinarily broad production this early in the case would pose numerous other problems. Some of the investigations may not be public, and Facebook may be under legal obligations or have agreements with regulators not to disclose those investigations. Even for investigations that are public, regulators may want documents produced in the investigations to be kept private. Facebook may need time to inform investigators of any request and determine how it may proceed. The Court might also need to set up a process for regulators to object to the discovery, perhaps anonymously. *See, e.g.*, *In re Capacitors Antitrust Litig.*, No. 14-CV-03264-JD, Dkt. 309 (N.D. Cal. Oct. 30, 2014); *In re Sulfuric Acid Antitrust Litig.*, 2004 WL 769376, at *5 (N.D. Ill. Apr. 9, 2004).

Courts have been especially wary of disrupting foreign investigations. Courts must undertake a comity analysis before ordering production that may interfere with another sovereign's investigation.

See In re Rubber Chem. Antitrust Litig., 486 F. Supp. 2d 1078, 1081–84 (N.D. Cal. 2007); *Campbell v. Facebook Inc.*, 2015 WL 4463809, at *2–3 (N.D. Cal. July 21, 2015). Even if the "documents are plainly relevant," comity may trump civil discovery. *In re Payment Card Interchange Fee & Merch. Disc. Antitrust Litig.*, 2010 WL 3420517, at *5–9 (E.D.N.Y. Aug. 27, 2010); *accord*, *e.g.*, *In re Cathode Ray Tube (CRT) Antitrust Litig.*, 2014 WL 6602711, at *3 (N.D. Cal. Nov. 20, 2014).

There is no need to wade into any of these issues before Plaintiffs have even filed a consolidated complaint, particularly given the serious questions surrounding whether they can plead any viable theory against Facebook (and they cannot). Plaintiffs "seek production of documents (not testimony) already compiled and turned over to the government," so "[t]here is little to no risk that these documents will be unavailable in the future." *In re Vioxx Prods. Liab. Litig.*, 2008 WL 1995098, at *4 (E.D. La. May 6, 2008); *In re White*, 2010 WL 1780234, at *2 (S.D. Miss. May 3, 2010); *In re Wholesale Grocery Prods. Antitrust Litig.*, 2010 WL 11469883, at *3 (D. Minn. Mar. 3, 2010). Because Plaintiffs cannot show prejudice, their "request for early discovery as to materials a party has provided to a government entity as part of an ongoing investigation" must be denied. *In re Domestic Airline Travel Antitrust Litig.*, 174 F. Supp. 3d 375, 376 (D.D.C. 2016).

4. Plaintiffs' desire for a fishing expedition is not a proper basis for early discovery

Plaintiffs candidly acknowledge their purpose in seeking broad discovery at this early stage: they seek insight into what they "do not know, but wish to know, before filing a pleading." Mem. at 11. In other words, they want to obtain confidential internal Facebook documents first, and then see what legal theory they might come up with. That would turn the Federal Rules on their head. "[A]llowing plaintiffs to file first and investigate later … would be contrary to Rule 11(b)[(3)], which mandates an 'inquiry reasonable under the circumstances' into the evidentiary support for all factual contentions prior to filing a pleading." *Timmons v. Linvatec Corp.*, 263 F.R.D. 582, 585 (C.D. Cal. 2010). It is up to *Plaintiffs' counsel* to investigate the "evidentiary support for all factual contentions prior to filing a pleading"; they cannot use Facebook to conduct the investigation for them. *Id.*; *see also Am. LegalNet, Inc. v. Davis*, 673 F. Supp. 2d 1063, 1069 (C.D. Cal. 2009); *In re Fannie Mae Deriv. Litig.*, 227 F.R.D. 142, 143 (D.D.C. 2005). Accordingly, courts consistently reject attempts to conduct discovery before filing suit because "ascertain[ing] facts for the use in framing a complaint" is not a proper use of early

discovery. *In re Solorio*, 192 F.R.D. 709, 709–10 (D. Utah 2000); *accord*, *e.g.*, *Vioxx*, 2008 WL 1995098, at *6 (denying party in MDL discovery "meant to discover facts in order to determine whether it has a claim"). Such "pre-suit discovery" supposedly "necessary in order for [plaintiffs] to be able to bring an action … is simply not authorized" by the Federal Rules. *White*, 2010 WL 1780234, at *2.

Plaintiffs argue that their request to put the discovery cart before the horse "would allow this litigation to proceed more speedily." Mem. at 12. But it would "always be more efficient—at least from a plaintiff's perspective—to obtain discovery" early in the litigation. *Megaupload, Ltd. v. Universal Music Grp., Inc.*, 2012 WL 243687, at *3 (N.D. Cal. Jan. 25, 2012). "Nonetheless, the federal rules, adopted after much study and thought, dictate a different procedure." *Id.*; *see also Hall v. Mims*, 2012 WL 1498893, at *3 (E.D. Cal. Apr. 27, 2012); *St. Louis Grp., Inc. v. Metals & Additives Corp.*, 275 F.R.D. 236, 240–41 (S.D. Tex. 2011); *Flash Memory*, 2008 WL 62278, at *5.

Although Plaintiffs claim that "courts commonly order the production of documents before a consolidated complaint is filed," the unpublished minute orders they cite in support of that proposition do not back up that claim. Indeed, in *In re High Tech Employee Antitrust Litig.*, No. 5:11-cv-02509-LHK, Dkt. 88 (N.D. Cal. Oct. 26, 2011), a defendant had already filed a motion to dismiss the consolidated complaint *more than a month before* the discovery order Plaintiffs cite. *See id.*, Dkt. 79. Other cases appear to have involved voluntary productions; in *In re Resistors Antitrust Litig.*, No. 5:15-cv-03820-RMW, Dkt. 112 (N.D. Cal. Feb. 2, 2016), the minute order noted that the defendants would "*voluntarily* produce[]" documents to the plaintiffs, and the court later ordered a stay of discovery at the request of the Department of Justice, *see id.*, Dkt. 120. Likewise, in *In Re: 21st Century Oncology Customer Data Security Breach Litig.*, No. 8:16-md-2737, Dkt. 81 (M.D. Fla. Nov. 18, 2016), the parties *agreed* to produce pre-complaint discovery. *See id.*, Dkt. 83, at 21–22. The order in *In re Liquid Aluminum Sulfate Antitrust Litig.*, No. 16-md-2687, Dkt. 209 (D.N.J. July 5, 2016), is similarly distinguishable. There, the court ordered production of documents related to a single investigation—not numerous state, federal, and foreign investigations, and sprawling additional discovery, as Plaintiffs seek—and the court otherwise directed that discovery be stayed. *See id.*

The only other orders Plaintiffs cite in which a court required production of discovery before

the filing of a consolidated complaint did not analyze whether the Federal Rules permit such a sequence, or acknowledge any of the cases ruling otherwise. *See In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prods. Liab. Litig.*, No. 10-ml-2151, Dkt. 180 (C.D. Cal. June 1, 2010); *In re Lithium Ion Batteries Antitrust Litig.*, 2013 WL 2237887, at *3 (N.D. Cal. May 21, 2013). Nothing in those cases upsets the well-reasoned analysis in *Flash Memory* explaining why the filing of a consolidated complaint must precede discovery. And neither case involved fundamental uncertainty about whether the plaintiffs could even plead a viable claim, as this case does.

Facebook is aware of no reported decision allowing pre-complaint discovery under these circumstances, where Plaintiffs' anticipated theories rest on such unstable footing and where no consolidated complaint has been filed. Permitting this massive discovery before Plaintiffs have articulated their claims would exceed the discretion afforded courts and would constitute error.

IV. CONCLUSION

For the foregoing reasons, Facebook respectfully requests that this Court stay all discovery pending resolution of Facebook's Motion to Dismiss.

DATE: August 15, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER, LLP

By: */s/ Joshua S. Lipshutz*

Joshua S. Lipshutz (SBN 242557)
jlipshutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Telephone: 202.955.8500
Facsimile: 202.467.0539

Orin Snyder (*pro hac vice pending*)
osnyder@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, NY 10166-0193
Telephone: 212.351.4000
Facsimile: 212.351.4035

Kristin A. Linsley (SBN 154148)
klinsley@gibsondunn.com
Brian M. Lutz (SBN 255976)
blutz@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
555 Mission Street, Suite 3000
San Francisco, CA 94105-0921
Telephone: 415.393.8200
Facsimile: 415.393.8306

Attorneys for Defendant Facebook, Inc.

APPENDIX

Flaws in Plaintiffs' Primary Causes of Action[1]

Federal Wiretap Act
Elements/Legal Principles: • Unlawful to "intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). • "[T]o be 'intercepted' in violation of the Wiretap Act, [information] must be acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002). ***Flaws***: • Plaintiffs' claims that information they stored on Facebook was improperly accessed by Facebook or Cambridge Analytica are governed by the Stored Communications Act ("SCA"), not the Wiretap Act. *See id.* (narrow definition of "intercept" excluding stored communications "is consistent with the structure of the ECPA, which created the SCA for the express purpose of addressing 'access to *stored* … electronic communications and transactional records'" (quoting S. Rep. No. 99–541 at 3)). • It would not have been unlawful for Facebook to obtain users' communications while in transmission because Facebook was a party to those communications. It is not "unlawful … for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication." *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017) (emphasis and internal citation omitted). Facebook is a "party to" content shared by users on Facebook. *See id*. • Plaintiffs authorized Facebook to collect the information at issue by agreeing to Facebook's Data Use Policy. *See* Ex. C.

Stored Communications Act
Elements/Legal Principles: • SCA § 2701(a) prohibits accessing a facility through which an electronic service is provided without authorization or in excess of an authorization. • SCA § 2702(a) limits the ways in which electronic service providers ("ESPs") may disclose customer communications to third-parties, but permits ESPs to disclose customer communications "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service." 18 U.S.C. § 2702(b)(3). • "[T]he question at the motion to dismiss phase is whether plaintiffs have plausibly alleged that a reasonable user who undertook [the service provider's] process has not consented to the [disclosure]." *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1214 (N.D. Cal. 2014). • In assessing whether users of social media and electronic communication services have "consented" to disclosures, courts examine the ESP's terms of service and privacy policies. *See id*. at 1212–14; *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1028–29 (N.D. Cal 2014).

[1] This Appendix is based on claims pled to date and is not intended to be an exhaustive list of possible defenses or flaws in Plaintiffs' forthcoming consolidated class action complaint.

Flaws:

- Facebook's policy of allowing users to share their friends' information with apps, in line with those friends' privacy settings, did not violate § 2702(a) because both the person sharing the information and the friend using the app consented—the former because Facebook's Data Use Policy disclosed to users that their friends could share some of their information with apps they used, and the latter, who were "intended recipients" under the SCA, by affirmatively authorizing third-party apps to access their and their friends' data (subject to applicable privacy settings).
- Any SCA claims fail to the extent they relate to disclosure of "record" information, rather than content of users' communications. Section 2702(c)(6) permits an electronic service provider to "divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by [§ 2702](a)(1) or (a)(2)) … to any person other than a governmental entity." 18 U.S.C. 2702(c)(6). A "record" includes "among other things, the 'name,' 'address,' and 'subscriber number or identity' of 'a subscriber to or customer of such service,'" and a "Facebook ID" is a "record" under this definition. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1104 (9th Cir. 2014).

Common-Law Negligence

Elements/Legal Principles:

- "As a general rule, one owes no duty to control the conduct of another, nor to warn those endangered by such conduct." *Davidson v. City of Westminster*, 32 Cal. 3d 197, 203 (1982). Courts in this District have held that there is no independent legal duty "to protect users' personal information from third-party app developers." *Pirozzi v. Apple Inc.*, 913 F. Supp. 2d 840, 852 (N.D. Cal. 2012); *In re iPhone Application Litig.*, 2011 WL 4403963, at *9 (N.D. Cal. Sept. 20, 2011); *In re Google Android Consumer Privacy Litig.*, 2013 WL 1283236, at *13 (N.D. Cal. Mar. 26, 2013).
- A plaintiff cannot recover in tort solely on a theory that a contract was negligently performed absent some independent tort duty. *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 514–15 (1994).
- In California, "[g]enerally speaking, in actions for negligence, liability is limited to damages for physical injuries and recovery of economic loss is not allowed. In the absence of (1) personal injury, (2) physical damage to property, (3) a 'special relationship' existing between the parties, or (4) some other common law exception to the rule, recovery of purely economic loss is foreclosed." *Kalitta Air, L.L.C. v. Cent. Tex. Airborne Sys., Inc.*, 315 F. App'x 603, 605 (9th Cir. 2008) (citations omitted). Numerous courts have held that the rule bars claims that closely resemble those at issue here. *See, e.g.*, *In re Lenovo Adware Litig.*, 2016 WL 6277245, at *10 (N.D. Cal. Oct. 27, 2016); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1054–55 (N.D. Cal. 2014); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 967–73 (S.D. Cal. 2014); *Google Android Consumer Privacy Litig.*, 2013 WL 1283236, at *12–*13; *iPhone Application Litig.*, 844 F. Supp. 2d at 1064.

Flaws:

Facebook's relevant Data Use Policy states that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook, so you should always make sure to read their terms of service and privacy policies to understand how they treat your data." Ex. C at 8 [2013 Data Use Policy].

Facebook has not breached any legal duty it owes to anyone.

- To the extent Plaintiffs rely on contractual duties, those duties cannot support a negligence claim.

- The economic loss rule bars tort recovery in this case because Plaintiffs do not allege personal injury or physical damage to property, and cannot allege that they were in a "special relationship" with Facebook. "[A] critical foundational requirement for finding a special relationship is whether the third-party transaction was intended to affect the plaintiff in a particular way." *Platte Anchor Bolt, Inc. v. IHI, Inc.*, 352 F. Supp. 2d 1048, 1054 (N.D. Cal. 2004). Businesses do not share a special relationship with ordinary buyers of their products who are "no different from any other purchaser of the *same product*." *Greystone Homes, Inc. v. Midtec, Inc.*, 168 Cal. App. 4th 1194, 1230–31 (2008); *see also Ott v. Alfa-Laval Agri, Inc.*, 31 Cal. App. 4th 1439, 1455–56 (1995). Plaintiffs do not have any "'special relationship' with [Facebook] beyond those envisioned in everyday consumer transactions, and therefore, negligence is the wrong legal theory on which to pursue recovery for Plaintiffs' economic losses." *In re Sony*, 996 F. Supp. 2d at 969; *see also Stewart v. Electrolux Home Prods., Inc.*, 2018 WL 339059, at *4 (E.D. Cal. Jan. 9, 2018).
- The lack of actionable harm also bars any negligence claim. "Under California law, appreciable, nonspeculative, present harm is an essential element of a negligence cause of action." *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 962 (S.D. Cal. 2012). "The breach of a duty causing only speculative harm or the threat of future harm does not normally suffice to create a cause of action." *Aas v. Superior Court*, 24 Cal. 4th 627, 646 (2000). Courts in data misuse cases consistently have dismissed such claims for want of sufficient allegations of harm. *See Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (insufficient harm where plaintiff "spent time, money, energy, and effort managing the fallout" after an unknown party attempted to make fraudulent transactions in his name); *In re iPhone I*, 2011 WL 4403963, at *9 (dismissing negligence claim for lack of "appreciable, nonspeculative, present injury"); *In re iPhone II*, 844 F. Supp. 2d at 1064 (dismissing negligence claim where alleged harms were "either too speculative to support a claim for negligence under California law, or they stem from disappointed expectations from a commercial transaction and thus do not form the basis of a negligence claim."); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1032 (N.D. Cal. 2012) (dismissing negligence claim because plaintiffs failed to explain how they were foreclosed from capitalizing on their personal data or if any third party actually obtained de-anonymized data).

Privacy Claims under the California Constitution

Elements/Legal Principles:

- To make out an invasion of privacy claim under Article I, Section 1 of the California Constitution "the complaining party must … demonstrate (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Lewis v. Superior Court*, 3 Cal. 5th 561, 571 (2017) (citations omitted).

Flaws:

- Plaintiffs' claimed general privacy interest in "their online behavior on Facebook," *see, e.g.*, Beiner Compl. ¶ 115, is insufficient because it fails to specify exactly what protected information was disseminated. *See In re Yahoo*, 7 F. Supp. 3d at 1041 (dismissing privacy claims where plaintiff failed to allege contents of emails); *Zbitnoff v. Nationstar Mortg., LLC*, 2014 WL 1101161, at *4 (N.D. Cal. Mar. 18, 2014) (dismissing privacy claims against mortgage company that allegedly disseminated private information to third parties for credit checks where plaintiff failed to allege what specific information was improperly disseminated); *Scott-Codiga v. Cty. of Monterey*, 2011 WL 4434812, at *7 (N.D. Cal. Sept. 23, 2011) (plaintiff failed to specify what private facts the defendants allegedly disclosed to the public).

- Plaintiffs have consented to disclosure of the data at issue. "Even when a legally cognizable privacy interest is present … advance notice of an impending action may serve to limit [an] intrusion upon personal dignity and security that would otherwise be regarded as serious." *Hill*, 7 Cal. 4th at 36 (quotation marks and citation omitted). "If the undisputed material facts show no reasonable expectation of privacy or an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law." *Id.* One does not have an objectively reasonable expectation of privacy in information he has consented to disclose. *See, e.g., Yahoo*, 7 F. Supp. 3d at 1037–38 ("voluntary consent" defeats privacy claim).

- Plaintiffs agreed to Facebook's Data Use Policy, which authorized their friends to re-share information with apps in line with their privacy settings. Plaintiffs also had the ability to change their privacy settings to limit what information apps could access.

- No serious invasion of privacy is alleged here. "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious *breach* of the social norms underlying the privacy right." *Hill*, 7 Cal. 4th at 37. "[R]outine commercial behavior" does not constitute an "egregious breach of … social norms," *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (2011), and "[e]ven disclosure of very personal information has not been deemed an 'egregious breach of social norms' sufficient to establish a constitutional right to privacy." *Yahoo*, 7 F. Supp. 3d at 1038.

- Allegations that a company failed to secure consumers' personal information not an "egregious breach of social norms." *See, e.g.*, *Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) (no invasion of privacy where hackers obtained plaintiff's social security number and someone tried to open a credit card in the plaintiff's name); *In re Google Android Cons. Privacy Litig.*, 2013 WL 1283236, at *11 (N.D. Cal. Mar. 26, 2013) (no invasion of privacy where Google's conduct allowed third parties to obtain plaintiffs' PII, transmit it without encryption, and track PII over a substantial period of time); *Gonzales*, 1863148305 F. Supp. 3d at 1092–93 (no invasion of privacy where Uber obtained plaintiff's name and home address); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (no invasion of privacy where Pandora obtained personal information "and provided that information to advertising libraries for marketing purposes" in violation of its privacy policy); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1063 (disclosure to third parties of unique device identifier number, personal data, and geolocation information was not invasion of privacy); *Low*, 900 F. Supp. 2d at 1025 (no invasion of privacy where LinkedIn disclosed to third parties users' numeric LinkedIn ID and LinkedIn browsing histories).

Common-Law Intrusion

Elements:

- "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." *Shulman v. Grp. W Prods., Inc.*, 18 Cal. 4th 200, 231 (1998).

- "The tort is proven only if the plaintiff had an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source." *Id*. at 232.

Flaws:

- Plaintiffs consented to the sharing of data with apps their friends used.

Contract Claims

Elements/Legal Principles:

- "Under California law, to state a claim for breach of contract a plaintiff must plead the contract, plaintiffs' performance (or excuse for nonperformance), defendant's breach, and damage to plaintiff therefrom." *Low*, 900 F. Supp. 2d at 1028.

- *Breach*: Plaintiff must "allege the specific provisions in the contract creating the obligation the defendant is said to have breached." *Young v. Facebook, Inc.*, 790 F. Supp. 2d 1110, 1117 (N.D. Cal. 2011); *see also Frances T. v. Vill. Green Owners Ass'n*, 42 Cal. 3d 490 (1986) (plaintiff must allege that some provision in a relevant writing imposed the alleged duty on the defendant").

- *Damages*: "Under California law, a breach of contract claim requires a showing of appreciable and actual damage." *Aguilera v. Pirelli Armstrong Tire Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000); *St. Paul Fire and Marine Ins. Co. v. American Dynasty Surplus Lines Ins.*, 101 Cal. App. 4th 1038, 1060 (2002) ("An essential element of a claim for breach of contract are damages resulting from the breach."). "Actual damage as opposed to mere nominal damages" are required, *Roberts v. L.A. Cty. Bar Ass'n*, 105 Cal. App. 4th 604, 617 (2003), and "[e]motional and physical distress damages are not recoverable." *Low*, 900 F. Supp. 2d at 1028; *see also Frangipani v. Boecker*, 64 Cal. App. 4th 860, 865 (1998) ("[T]he invariable rule [is] pronounced by a legion of cases that damages are not recoverable for mental suffering or injury to reputation resulting from breach of contract.").

Flaws:

- Plaintiffs cannot allege breach. Plaintiffs assert that Facebook had an obligation to prevent Cambridge Analytica from obtaining and misusing their data. No provision of the Data Use Policy or SRR creates such a legal obligation and the terms of the agreements state otherwise. Plaintiffs agreed that friends could share their information with apps. The SRR contained a waiver of any claims "arising out of or in any way connected with any claims [users] have against … third parties." Ex. D at 4. And the Data Use Policy in effect at the relevant time informed users that "games, applications and websites are created and maintained by other businesses and developers who are not part of, or controlled by, Facebook," and that "how they treat your data" is governed by "their terms of service and privacy policies." Ex. C at 8.

- Plaintiffs have not suffered contract damages—*i.e.,* that disclosure of their information caused them any economic harm. *See Folgelstrom*, 195 Cal. App. 4th at 994 ("The fact that the [plaintiff's] address had value to [the defendant], such that the retailer paid … a license fee for its use, does not mean that its value to plaintiff was diminished in any way.").

The California Unfair Competition Law

Elements/Legal Principles:

- To have statutory standing under the UCL an individual must "ha[ve] suffered injury in fact and ha[ve] lost money or property as a result of the unfair competition." Cal. Bus. & Prof.

Code § 17204; *see Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310 (2011). This requirement is "more stringent than the federal standing requirements." *Troyk v. Farmers Group, Inc.*, 171 Cal. App. 4th 1305, 1348 fn. 31 (2009). "Whereas a federal plaintiff's 'injury in fact' may be intangible and need not involve lost money or property, Proposition 64, in effect, added a requirement that a UCL plaintiff's 'injury in fact' specifically involve 'lost money or property.'" *Id*.

- "A UCL action is an equitable action by means of which a plaintiff may recover money or property obtained from the plaintiff or persons represented by the plaintiff through unfair or unlawful business practices. It is not an all-purpose substitute for a tort or contract action." *Cortez v. Purolator Air Filtration Prod. Co.*, 23 Cal. 4th 163, 173 (2000). "[D]amages are not available" in a UCL action. *Id*.; *see also Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1144 (2003) ("A UCL action is equitable in nature; damages cannot be recovered."); *Kraus v. Trinity Mgmt. Servs., Inc.*, 23 Cal. 4th 116, 137 (2000) (UCL "does not authorize orders for disgorgement into a fluid recovery fund").

Flaws:

- Plaintiffs cannot allege economic injury under a "benefit of the bargain" theory because they did not pay for Facebook's services. *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 966 (S.D. Cal. 2012) ("[p]laintiffs have not alleged 'lost money or profits'" where they "received the … services free of cost"); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 714-15 (N.D. Cal. 2011) (where plaintiffs received Facebook's services for free, "as a matter of law, Plaintiffs cannot state a UCL claim under their own allegations."); *In re Yahoo!*, 2018 WL 1243332, at *9 (dismissing claims brought by non-paying users for failure to demonstrate economic injury, but allowing paid user claim to proceed on "lost benefit of the bargain" theory).

- Plaintiffs cannot allege standing under the UCL based on the purported diminution in value of their personal information because "a plaintiff's 'personal information' does not constitute money or property under the UCL." *In re iPhone Application Litig.*, 2011 WL 4403963, at *14; *see, e.g.*, *Sony*, 903 F. Supp. 2d at 966 (the loss of "property value in one's information, do[es] not suffice as injury under the UCL"); *Yunker v. Pandora Media, Inc.*, 2013 WL 1282980, at *4 (N.D. Cal. Mar. 26, 2013) (plaintiff failed to demonstrate Article III "injury-in-fact" "based on the purported diminution in value of his PII"); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 714-15 (personal information does not "constitute[e] property for purposes of a UCL claim").

- Because Plaintiffs cannot allege a credible risk of identity theft, they cannot plausibly claim that Facebook's conduct caused them to purchase identity theft monitoring services. *See Sony*, 903 F. Supp. 2d at 966 ("Plaintiffs' allegations that the heightened risk of identity theft, time and money spent on mitigation of that risk … do not suffice as injury under the UCL"); *Corona v. Sony Pictures Entm't, Inc.*, 2015 WL 3916744, *5 (C.D. Cal. June 15, 2015) (finding sufficient injury where plaintiffs purchased monitoring services after the public disclosure of "Social Security numbers, employment files, salary and bank account information, health insurance and other medical information, names, home and email addresses, visa and passport numbers, and retirement plan data").

- Plaintiffs have not alleged that Facebook took any money or property from them or identified any money or property in Facebook's possession that could be returned to them as restitution.

- Any UCL claim would also fail because Facebook's conduct was not fraudulent, unlawful, or unfair. The practices Plaintiffs complain of were disclosed to them and did not violate any statute.